(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－269375
（P2002－269375A）
(43)公開日　平成14年９月20日(2002.9.20)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　17/60	３０２	Ｇ０６Ｆ　17/60	３０２Ｅ　５Ｊ１０４
	ＺＥＣ		ＺＥＣ
	３３２		３３２
	４００		４００
	５１２		５１２

審査請求　未請求　請求項の数15　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願2001－70580(P2001－70580)

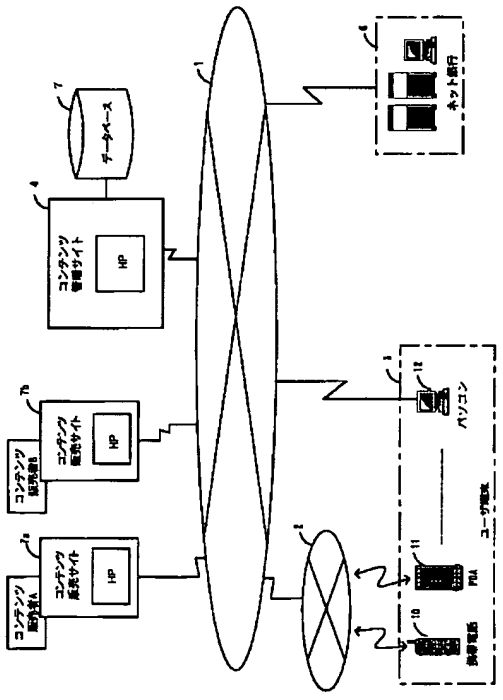
(22)出願日　平成13年３月13日(2001.3.13)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　永井　規浩
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100097216
弁理士　泉　和人　（外１名）

Ｆターム(参考)　5J104 AA01 AA16 EA04 EA18 NA02 NA05 PA09

(54)【発明の名称】　コンテンツ管理方法およびシステム

(57)【要約】
【課題】　ユーザがコンテンツ供給サイトから容易に確実に安全にコンテンツを購入して使用できるコンテンツ管理方法およびシステムを提供する。
【解決手段】　ユーザ端末３からコンテンツ管理サイト４にユーザ登録を行い、ユーザは、コンテンツ管理サイト４のホームページでコンテンツを閲覧して購入し、この購入代金がネット銀行を介して支払われる。コンテンツ管理サイト４は、コンテンツをデータベース８に登録し、情報の使用権とコンテンツをユーザ端末に送信する。この移動された使用権に基づいて、ユーザ端末はコンテンツを取り込んで利用する。ユーザ端末は、コンテンツの使用権をコンテンツ管理サイト４に戻し、かつ、保持しているコンテンツを消去することができる。ユーザは、使用権に基づいてコンテンツ管理サイト４から再度情報を取り込んで利用することができる。



1

【特許請求の範囲】

【請求項１】　コンテンツ供給サイト、コンテンツ管理サイトおよびユーザ端末とを備え、コンテンツの購入の斡旋および購入されたコンテンツの管理を行うコンテンツ管理方法において、

ユーザ端末が、コンテンツ供給サイトにユーザ登録を行うステップと、

コンテンツ供給サイトが、ユーザ端末に対してコンテンツ内容を提示するステップと、

ユーザ端末が、コンテンツ供給サイトからコンテンツを購入するステップと、

ユーザ端末がコンテンツ供給サイトに購入したコンテンツの代金を支払うステップと、

コンテンツ供給サイトが、ユーザ端末が購入した情報をコンテンツ管理サイトのデータベースに登録するステップと、

コンテンツ供給サイトが、データベースに登録しているコンテンツ使用権をユーザ端末に移動させるステップと、

ユーザ端末が、コンテンツ供給サイトからコンテンツ使用権に基づいてコンテンツを取り込むステップと、を有することを特徴とするコンテンツ管理方法。

【請求項２】　前記ユーザ端末は、取り込んだコンテンツ使用権をコンテンツ管理サイトに戻すと共にユーザ端末で取り込んだ情報を消去するステップをさらに有することを特徴とする請求項１記載のコンテンツ管理方法。

【請求項３】　前記ユーザ端末は、コンテンツ使用権に基づいて、前記でコンテンツ管理サイトに戻されたコンテンツを取り込むステップをさらに有することを特徴とする請求項２記載のコンテンツ管理方法。

【請求項４】　コンテンツ供給サイトが、ユーザ端末に対してコンテンツ内容を提示する内容は、少なくとも購入を勧めるコンテンツリストおよびコンテンツ内容であることを特徴とする請求項１記載のコンテンツ管理方法。

【請求項５】　ユーザ端末が前記コンテンツ供給サイトにユーザ登録を行うステップにおいて、

ユーザ識別符号およびパスワードと共に、少なくともダイレクトマーケティング用にユーザの各種個人情報を登録することを特徴とする請求項１記載のコンテンツ管理方法。

【請求項６】　前記コンテンツ管理サイトは、ユーザ端末がコンテンツ管理サイトからコンテンツを取り込むときに、広告を含む情報をコンテンツに添付するステップをさらに有することを特徴とする請求項１記載のコンテンツ管理方法。

【請求項７】　前記使用権の情報は、前記コンテンツ供給サイトとユーザ端末との間で、ユーザ登録における識別符号およびパスワードと共に、暗号化して送信されることを特徴とする請求項１記載のコンテンツ管理方法。

2

【請求項８】　前記暗号化はＡＫＥ(Authentication And Key Exchange) プロトコルが適用されることを特徴とする請求項７記載のコンテンツ管理方法。

【請求項９】　コンテンツ供給サイト、コンテンツ管理サイトおよびユーザ端末とを備え、コンテンツの購入の斡旋および購入されたコンテンツの管理を行うコンテンツ管理システムにおいて、

前記コンテンツ供給サイトはコンテンツを蓄積し、要求に基づいてコンテンツ管理サイトに供給し、

前記ユーザ端末は、コンテンツを購入するためのユーザ登録を行うと共に、購入したコンテンツの使用権と共にコンテンツを取り込み、さらに、コンテンツの使用権に基づいて再度コンテンツを取り込み、

コンテンツ管理サイトは、前記ユーザ端末がユーザ登録をしたときに、コンテンツ供給サイトからコンテンツを取り込んで記憶し、ユーザ端末からの要求に基づいてコンテンツ使用権を前記ユーザ端末に移動すると共に前記記憶したコンテンツを前記ユーザ端末に供給することを特徴とするコンテンツ管理システム。

【請求項１０】　前記ユーザ端末は、取り込んだコンテンツ使用権をコンテンツ管理サイトに戻すと共にユーザ端末で取り込んだ情報を消去することを特徴とする請求項９記載のコンテンツ管理システム。

【請求項１１】　前記ユーザ端末は、前記でコンテンツ管理サイトに戻されたコンテンツを、さらに、コンテンツ使用権と共に取り込むことを特徴とする請求項１０記載のコンテンツ管理システム。

【請求項１２】　前記ユーザ端末とコンテンツ管理サイトとの間、または前記ユーザ端末とコンテンツ供給サイトとの間で代金決済を行うためのネット代金決済手段を、さらに備えることを特徴とする請求項９記載のコンテンツ管理システム。

【請求項１３】　前記コンテンツ管理サイトは、前記ユーザ端末が前記コンテンツ供給サイトにユーザ登録を行うときに、ユーザ識別符号およびパスワードと共に、少なくともダイレクトマーケティング用にユーザの各種個人情報を登録することを特徴とする請求項９記載のコンテンツ管理システム。

【請求項１４】　前記コンテンツ管理サイトは、前記ユーザ端末が前記コンテンツ管理サイトからコンテンツを取り込むときに、広告を含む情報をコンテンツに添付することを特徴とする請求項９記載のコンテンツ管理方法。

【請求項１５】　前記コンテンツ管理サイトは、少なくとも、コンテンツおよびコンテンツの使用権を格納するためのデータベースを備えることを特徴とする請求項９記載のコンテンツ管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＴＣＰ／ＩＰ環境

下の通信ネットワーク（イントラネット、インターネット、エキストラネット、ＵＮＩＸ（登録商標）ワークステーション、以下、インターネットという）を通じて、情報（例えば、音楽、静止画、動画などのコンテンツ内容、以下、コンテンツという）の購入の斡旋、および購入されたコンテンツの使用を管理するための、コンテンツ管理方法およびシステムに関する。

【０００２】

【従来の技術】従来、ＴＣＰ／ＩＰ環境下の通信ネットワークにおいて、音楽、静止画、動画のコンテンツなどが提供される。このコンテンツは、ウェブブラウザを搭載したユーザ端末（小型汎用コンピュータやインターネットサーフィンが可能な携帯端末）でダウンロードして利用される。

【０００３】このコンテンツをウェブサイトで提供する場合およびユーザが利用する場合には、著作権保護の立場から、ユーザサイトに、著作権モジュールを格納したソフトウェアが用いられている。このような著作権モジュールでダウンロードされるコンテンツ使用権は、ダウンロードを実行したユーザ端末にバインドされる。

【０００４】

【発明が解決しようとする課題】このようなウェブサイトを通じてコンテンツを提供し、その著作権を管理する立場のコンテンツ提供サイト、およびコンテンツを取得して利用するユーザ端末では、それぞれ次のような問題点がある。

【０００５】（１）コンテンツ提供サイト

（ａ）不特定多数のユーザに情報を提供するウェブサイトが、コンテンツを提供する場合に、そのユーザへの広告（例えば、雑誌広告や検索エンジンバナー広告）を含む管理に多大な時間や費用を要する。

（ｂ）ユーザが複数の端末を使用している場合、著作権の関係から個々のユーザ端末ごとに音楽などをダウンロードしなければならない。換言すれば、ユーザ端末に手間と費用の負担を強いることになり、結果的にコンテンツを普及させる阻害要因となる。

【０００６】（２）ユーザ端末

（ａ）一人のユーザが所有している複数の端末で同一のコンテンツを利用する場合、その複数の端末のそれぞれにおいて、同一のコンテンツをウェブサイトからダウンロードして使用することになる。この場合、操作が面倒であり、そのダウンロード費用なども嵩むことになる。

【０００７】（ｂ）ユーザ端末の記憶容量が不足すると、新たなコンテンツをダウンロードするために、以前に保管しているコンテンツを削除する必要がある。また、ユーザ端末に異常が発生して保管しているコンテンツを再生できなくなることがある。この場合、ダウンロードしたコンテンツを記録媒体（外付けハードディスク装置、フロッピー（登録商標）ディスク、ＭＯなど）にバックアップする必要があり、または、再度のダウンロードを行うことになり、その手間と購入費用を要してしまう。

【０００８】（ｃ）インターネット上には、多種多様な数多いコンテンツを提供するウェブサイトがある。すなわち、ユーザが所望するコンテンツの入手先のウェブサイトが容易に判明しない。この場合、ユーザが専門雑誌を調べ、またはインターネットサーフィンによる検索・閲覧が必要となり、その手間がかかり、かつ、費用も嵩むことになる。

（ｅ）ユーザ端末に保管されるダウンロードされたコンテンツを、離れた場所、例えば、外出先で他のユーザ端末で取り込んで利用するのは困難であり、不便であった。

【０００９】本発明の目的は、このような従来技術における課題を解決するためになされものであり、コンテンツ提供サイトにおいては、コンテンツ購入の斡旋が容易にできると共に、ユーザ端末においては、購入したコンテンツ使用管理の使い勝手（利便性）が向上するコンテンツ管理方法およびシステムを提供することにある。

【００１０】

【課題を解決するための手段】上記課題を達成するために、請求項１記載の発明によれば、本発明は、コンテンツ供給サイト、コンテンツ管理サイトおよびユーザ端末とを備え、コンテンツの購入の斡旋および購入されたコンテンツの管理を行うコンテンツ管理方法において、ユーザ端末が、コンテンツ供給サイトにユーザ登録を行うステップと、コンテンツ供給サイトが、ユーザ端末に対してコンテンツ内容を提示するステップと、ユーザ端末が、コンテンツ供給サイトからコンテンツを購入するステップと、ユーザ端末がコンテンツ供給サイトに購入したコンテンツの代金を支払うステップと、コンテンツ供給サイトが、ユーザ端末が購入した情報をコンテンツ管理サイトのデータベースに登録するステップと、コンテンツ供給サイトが、データベースに登録しているコンテンツ使用権をユーザ端末に移動させるステップと、ユーザ端末が、コンテンツ供給サイトからコンテンツ使用権に基づいてコンテンツを取り込むステップとを有することを特徴とする。

【００１１】請求項２記載の発明によれば、本発明のユーザ端末は、取り込んだコンテンツ使用権をコンテンツ管理サイトに戻すと共にユーザ端末で取り込んだ情報を消去するステップをさらに有することを特徴とする。

【００１２】請求項３記載の発明によれば、本発明のユーザ端末は、コンテンツ使用権に基づいて、コンテンツ管理サイトに戻されたコンテンツを取り込むステップをさらに有することを特徴とする。

【００１３】請求項４記載の発明によれば、本発明のコンテンツ供給サイトが、ユーザ端末に対してコンテンツ内容を提示する内容は、少なくとも購入を勧めるコンテンツリストおよびコンテンツ内容であることを特徴とす

る。

【００１４】請求項５記載の発明によれば、本発明は、ユーザ端末がコンテンツ供給サイトにユーザ登録を行うステップにおいて、ユーザ識別符号およびパスワードと共に、少なくともダイレクトマーケティング用にユーザの各種個人情報を登録することを特徴とする。

【００１５】請求項６記載の発明によれば、本発明のコンテンツ管理サイトは、ユーザ端末がコンテンツ管理サイトからコンテンツを取り込むときに、広告を含む情報をコンテンツに添付するステップをさらに有することを特徴とする。

【００１６】請求項７記載の発明によれば、本発明の使用権の情報は、コンテンツ供給サイトとユーザ端末との間で、ユーザ登録における識別符号およびパスワードと共に、暗号化して送信されることを特徴とする。

【００１７】請求項８記載の発明によれば、本発明の暗号化はＡＫＥ(Authentication AndKey Exchange) プロトコルが適用されることを特徴とする

【００１８】請求項９記載の発明によれば、本発明は、コンテンツ供給サイト、コンテンツ管理サイトおよびユーザ端末とを備え、コンテンツの購入の斡旋および購入されたコンテンツの管理を行うコンテンツ管理システムにおいて、コンテンツ供給サイトはコンテンツを蓄積し、要求に基づいてコンテンツ管理サイトに供給し、前記ユーザ端末は、コンテンツを購入するためのユーザ登録を行うと共に、購入したコンテンツの使用権と共にコンテンツを取り込み、さらに、コンテンツの使用権に基づいて再度コンテンツを取り込み、コンテンツ管理サイトは、ユーザ端末がユーザ登録をしたときに、コンテンツ供給サイトからコンテンツを取り込んで記憶し、ユーザ端末からの要求に基づいてコンテンツ使用権をユーザ端末に移動すると共に前記記憶したコンテンツをユーザ端末に供給することを特徴とする。

【００１９】請求項１０記載の発明によれば、請求項９記載の発明のユーザ端末は、取り込んだコンテンツ使用権をコンテンツ管理サイトに戻すと共にユーザ端末で取り込んだ情報を消去することを特徴とする。

【００２０】請求項１１記載の発明によれば、請求項１０記載の発明のユーザ端末は、コンテンツ管理サイトに戻されたコンテンツを、さらに、コンテンツ使用権と共に取り込むことを特徴とする。

【００２１】請求項１２記載の発明によれば、請求項９記載の発明は、ユーザ端末とコンテンツ管理サイトとの間、またはユーザ端末とコンテンツ供給サイトとの間で代金決済を行うためのネット代金決済手段を、さらに備えることを特徴とする。

【００２２】請求項１３記載の発明によれば、請求項９記載の発明のコンテンツ管理サイトは、ユーザ端末がコンテンツ供給サイトにユーザ登録を行うときに、ユーザ識別符号およびパスワードと共に、少なくともダイレクトマーケティング用にユーザの各種個人情報を登録することを特徴とする。

【００２３】請求項１４記載の発明によれば、請求項９記載の発明のコンテンツ管理サイトは、ユーザ端末が前記コンテンツ管理サイトからコンテンツを取り込むときに、広告を含む情報をコンテンツに添付することを特徴とする。

【００２４】請求項１５記載の発明によれば、請求項９記載の発明のコンテンツ管理サイトは、少なくとも、コンテンツおよびコンテンツの使用権を格納するためのデータベースを備えることを特徴とする。

【００２５】

【発明の実施の形態】実施の形態１．次に、本発明の実施の形態１のコンテンツ管理方法およびシステムについて図面を参照して詳細に説明する。図１は本発明の実施の形態１におけるシステム構成を示すブロック図である。図１においては、本発明を実現するために、ＴＣＰ／ＩＰ環境下の通信ネットワーク（インターネット）の構成を有する。

【００２６】図１に示す通信ネットワークは、ＩＳＤＮ(Integrated Services Digital Network)のディジタル固定通信網１と共に、このディジタル固定通信網１に接続されたディジタル移動通信網２を有している。ディジタル移動通信網２は、図示しない基地局を有しており、この基地局には、インターネットアクセスが可能なウェブブラウザを搭載した多数の携帯電話機１０、ＰＤＡ(Personal Digital Assistant)１１などの携帯端末が無線で接続される。

【００２７】また、ディジタル固定通信網１には、コンテンツの管理およびコンテンツをユーザ端末が使用する権利（使用権）を管理するコンテンツ管理サイト４が接続される。コンテンツ管理サイト４にはコンテンツ等を記憶するデータベース８が接続される、さらに、ユーザが使用するパソコン１２と、以降で説明する各種の代金決済を実行するための銀行やクレジットカード会社などに設置されるネット代金決済通信手段としてのネット銀行６とが設けられる。

【００２８】さらに、図１に示す通信ネットワークには、コンテンツ管理サイト４からの要求に従って静止画、動画、音楽などのコンテンツを提供するコンテンツ販売者Ａ，Ｂが有するコンテンツ供給サイト７（７ａ，７ｂ）が設けられている。ここではコンテンツ供給サイト７は、都合上２つしか表示してないが、これらは２以上であってもよい。

【００２９】携帯端末３は、以降で詳細に説明するように、暗号化処理（たとえば、以下に詳細に説明するＡＫＥプロトコル）のモジュールが搭載される。このモジュールは、例えば、ディジタルシグナルプロセッサ（ＤＳＰ）やソフトウェアによって実現される。

【００３０】また、この携帯端末３では、ダウンロード

して入手したコンテンツを再生、例えば、ダウンロードした音楽データを再生し、かつ、コンテンツを管理するためのプログラムを格納しており、このプログラムは、コンテンツに関する指示処理などを容易にするためのＧＵＩ(Graphical User Interface)も備えている。

【００３１】以下、本発明のシステム構成の概要を簡単に説明する。図２は本発明のシステム構成の概要を説明するためのブロック図である。図２において、携帯端末３、コンテンツ管理サイト４、コンテンツ販売サイト５およびネット銀行６の接続関係が示される。

【００３２】携帯端末３は、コンテンツ管理サイト４との間で通信を行い、コンテンツ管理サイト４はコンテンツ供給サイト７との間で通信を行い、携帯端末３は料金決済をコンテンツ管理サイト４を介してネット銀行６との間で行う。

【００３３】コンテンツ管理サイト４は、（１）ユーザ情報管理部、（２）情報提供部、（３）リンク設定部、（４）代金決済部、（５）コンテンツ配信部、（６）データベース部等を含む。

＊【００３４】上述のように、本発明の主要処理は、コンテンツ管理サイト４で行われる。以下に、図２に示すコンテンツ管理サイト４の処理を図３から図５のシーケンス図を用いて詳細に説明する。

【００３５】＜ユーザ登録、コンテンツ購入および購入コンテンツデータベース登録＞図３は、ユーザ登録、コンテンツ購入および購入コンテンツデータベース登録処理のシーケンス図である。図３において、まず、ユーザ端末３は、コンテンツ管理サイト４にアクセスし、コンテンツ管理サイト４のホームページ上でユーザ情報を登録するための情報入力（たとえば、住所、氏名、個人の嗜好などの個人情報）を行う。コンテンツ管理サイト４は、ユーザ情報を登録する。ここで、ユーザ登録は、図２で説明したユーザ情報管理部で各種の項目が登録される。登録される項目の一例を表１示す。この項目は一例であり、他の項目を登録してもよい。

【００３６】

【表１】

項目	内容
ユーザID	ユーザーを一意に決定するためのID
ユーザパスワード	ログインするためのパスワード
コンテンツID	ユーザコンテンツを一意に決定するためのID
コンテンツ鍵	コンテンツを暗号化するための鍵
コンテンツ	コンテンツ鍵により暗号化されたコンテンツ
コンテンツ使用権移動チェックフラグ	コンテンツ使用権が移動できる状態にあるかどうかをチェックするためのフラグ

【００３７】さらに、ユーザ端末のユーザ毎のダイレクトマーケティング用情報をデータベース８に収集する事もできる。この収集情報によって、ユーザごとの個人情報が収集され、効果的なダイレクトマーケティングが可能になる。

【００３８】次に、コンテンツ管理サイト４は、販売するコンテンツ情報を、ホームページ（ＨＰ）上で提示する。このコンテンツ情報は、図２で説明した情報提供部で行う。ユーザ端末は、このホームページを閲覧する。

【００３９】この後、ユーザ端末から、所望のコンテンツ購入依頼の情報（例えば、商品コード）がユーザ識別符号およびパスワードと共に送信される。コンテンツ管理サイト４は、ユーザ識別符号およびパスワードを認識した際に、図２のリンク設定部でコンテンツ管理サイト４とコンテンツ販売サイト７とのリンクを張り、ユーザ端末３からの購入依頼をコンテンツ販売サイト７に送信する。

【００４０】購入依頼を受け取ったコンテンツ販売サイト７は、コンテンツの販売金額を、直接電子メールでユーザ端末３に通知する。なお、このコンテンツ代金請求通知は、コンテンツ販売サイト７からコンテンツ管理サイト４を介して、ユーザ端末３に行うようにしても良い。

【００４１】代金請求通知を受けたユーザ端末３は、図２で説明した代金決済部を介して、ネット銀行６とリンクを設定し、コンテンツ販売サイトへ７の送金を実行する。なお、この決済は、クレジットカードによって行うことも出来る。また、ユーザ端末３が直接ネット銀行６にリンクして、デビットカードや電子マネーの振替による決済を行うようにしても良い。

【００４２】この代金決済後に、コンテンツ販売サイト７は、購入されたコンテンツをコンテンツ管理サイト４に送信する。コンテンツ管理サイト４は、ユーザ端末３が購入したコンテンツを図２のデータベース部の処理によって、コンテンツ管理サイト４に置かれたデータベース８に格納する。この場合、購入コンテンツをユーザ識別符号およびパスワードに対応させてデータベース８に格納する。

【００４３】＜コンテンツ管理サイト４から携帯端末３へのコンテンツ使用権の移動＞図４は、コンテンツ管理サイト４から携帯端末３へコンテンツ使用権を移動するシーケンス図である。図４においては、コンテンツ管理

サイト４のデータベース８に格納されるユーザコンテンツおよびコンテンツ使用権をユーザ端末が取り込み、取り込んだコンテンツを携帯端末３が使用する処理の概要を示すものである。

【００４４】この処理においては、まず、ユーザ端末３からコンテンツ管理サイト４へログインが実行される。このログインでは、ユーザが、ユーザ端末３からコンテンツ管理サイト４にアクセスした後、コンテンツ管理サイト４のホームページ上で、ユーザ識別符号およびパスワードを入力する。

【００４５】コンテンツ管理サイト４は、ユーザ識別符号およびパスワードを正しく認識すると、データベース８上で保有しているユーザのコンテンツに関する情報（例えば、コンテンツ名、コンテンツ作成者、購入先、使用権の移動可否等）をユーザ端末３に送信する。ユーザ端末３は、画面に表示されたユーザコンテンツ情報から所望のコンテンツを選択し、選択されたコンテンツ選択情報をコンテンツ管理サイト４に送信する。

【００４６】次に、ユーザ端末３およびコンテンツ管理サイト４間で、たとえば、ＡＫＥプロトコルを利用した相互認証を実行して、セッション鍵を共有する処理を行う。このＡＫＥプロトコルの利用による相互認証については後述する。

【００４７】次に、コンテンツ管理サイト４では、生成されたセッション鍵で、ユーザコンテンツのコンテンツ鍵を暗号化する。この暗号化されたコンテンツ鍵およびコンテンツ鍵で暗号化されたコンテンツをユーザ端末に送信する。

【００４８】次に、ユーザ端末３では、暗号化されたコンテンツ鍵を、前記のコンテンツ管理サイト４と共有化したセッション鍵で復号化してコンテンツ鍵を取り出し、秘密鍵で再度暗号化して、ユーザ端末３内の図示しないメモリなどに記憶する。コンテンツ鍵で暗号化されたコンテンツもユーザ端末３内の図示しないメモリなどに記憶される。

【００４９】携帯端末３では、ユーザがメモリに記憶されたコンテンツを利用する。この場合、コンテンツは、ユーザ端末３に予めインストールされたユーザコンテンツ管理用ソフトウェア（プログラム）で再生される。このプログラムは、暗号化されたコンテンツ鍵を復号化し、この復号化で取得されたコンテンツ鍵を用いて、暗号化されたコンテンツを復号化して、コンテンツの画面表示や音楽出力などを行う。

【００５０】この結果、ユーザは、所有する複数のユーザ端末３に同一のコンテンツをダウンロードして使用する必要がなくなり、その手間および費用が削減される。

【００５１】さらに、ユーザ端末３は、コンテンツ管理サイト４を通じて購入したコンテンツ使用権を、離れた場所のユーザ端末で取り込んで利用できるようになる。

【００５２】＜携帯端末３からコンテンツ管理サイト４へのコンテンツ使用権の移動＞図５は携帯端末３からコンテンツ管理サイト４へのコンテンツ使用権の移動を示すシーケンス図である。図５においては、たとえば、ユーザ端末内のメモリの記憶容量が不足して、新たなコンテンツの取り込みが出来ない場合に、ユーザ端末３がコンテンツ管理サイト４から取り込んだコンテンツを削除して、コンテンツ使用権をコンテンツ管理サイト４に一時的に移動するものである。

【００５３】この処理においては、まず、ユーザ端末３からコンテンツ管理サイト４にログインが実行される。このログインでは、ユーザが、ユーザ端末３からコンテンツ管理サイト４にアクセスし、そのホームページ上でユーザ識別符号およびパスワードを入力する。

【００５４】コンテンツ管理サイト４は、このユーザ識別符号およびパスワードを正しく認識すると、データベース８上で保有しているユーザのコンテンツに関する情報をコンテンツ管理サイト４からユーザ端末３に送信する。ユーザ端末３では、画面表示したユーザコンテンツ情報から所望のコンテンツを選択し、選択されたコンテンツ選択情報をコンテンツ管理サイト４に送信する。

【００５５】次に、ユーザ端末３およびコンテンツ管理サイト４間で、たとえば、ＡＫＥプロトコルを利用した相互認証を実行して、セッション鍵を共有する処理を行う。このＡＫＥプロトコルの利用による相互認証については後述する。

【００５６】次に、携帯端末３では、生成されたセッション鍵で、ユーザコンテンツを一義的に決定するコンテンツ識別符号ＩＤを暗号化してコンテンツ管理サイト４に送信する。一方、コンテンツ管理サイト４はユーザ端末３に対してコンテンツ削除要求を送信する。

【００５７】このコンテンツ削除要求を受け取ったユーザ端末３は、内部のメモリなどに格納されたコンテンツ鍵およびコンテンツを削除する。

【００５８】このように、ユーザ端末３は、記憶容量が不足した場合に、格納しているコンテンツ使用権をコンテンツ管理サイト４に移動させ、かつ、格納しているコンテンツを削除することによって、新たなコンテンツのダウンロードが可能になる。

【００５９】実施の形態２．図６は本発明の他の実施の形態における処理の概略を説明するためのブロック図である。図６における処理では、情報添付サービスおよびダイレクトマーケティング情報を収集する。図６では、図２に示した（１）ユーザ情報管理部から（６）データベース部に加えて、新たに付加情報管理部およびダイレクトマーケティング情報収集部を含む。なお、図６では、コンテンツ管理サイト４は図２の処理に加えて次の処理を実行する。

＜付加情報管理＞コンテンツ管理サイト４は、コンテンツ供給サイト７から提供された情報、例えば、広告、コンテンツに関する付加情報をコンテンツ管理サイト４の

データベース８に格納する。コンテンツ管理サイト４は、付加情報管理部に格納された提供情報提を携帯端末３に配信されるコンテンツに添付して配信する。

【００６０】これによって、コンテンツ管理サイト４は、広告情報配信による収入が得られる。結果的にユーザのコンテンツ購入代金を低減できる。

【００６１】＜ダイレクトマーケティング情報の収集処理＞コンテンツ管理サイト４は、ユーザがコンテンツ管理サイト４を通じて購入するコンテンツの種類や、購入時期、購入時間帯などの情報を収集して、データベース８に格納する。

【００６２】なお、この購入時期、購入時間帯などの収集情報は、コンテンツ供給サイト７に供給され、またはコンテンツ管理サイト４で使用される。これによって。コンテンツ管理サイト４やコンテンツ供給サイト７は、ユーザが購入するコンテンツの傾向等を知ることができる。

【００６３】実施の形態３.

＜コンテンツ管理サイトとユーザ端末間の相手認証とセッション鍵の共有＞図７は、コンテンツ管理サイト４とユーザ端末３との間のＡＫＥプロトコルによる相手認証とセッション鍵の共有を詳細に説明するためのシーケンス図である。図７においては、ユーザ端末３は、第三者の証明機関によって発行されたユーザ証明書Cuserを、コンテンツ管理サイト４に送信する。コンテンツ管理サイト４は、ユーザ端末３からのユーザ証明書Cuserの正否を確認する。

【００６４】次に、コンテンツ管理サイト４は、ユーザ端末３に第三者の証明機関によって発行された証明書Cserverを送信する。ユーザ端末３は、証明書Cserverの正否を検証する。この検証が正しい場合にユーザ端末３は、証明書Cserverからコンテンツ管理サイト４の公開鍵e-serverを獲得する。次に、ユーザ端末３は乱数ｒ１を生成し、この乱数ｒ１は公開鍵e-serverを用いて暗号化される（Ｃ１＝Eserver（ｒ１）を生成する）。

【００６５】ユーザ端末３は、暗号化Ｃ１をコンテンツ管理サイト４に送信する。コンテンツ管理サイト４は、秘密鍵dserverを用いてｔ１＝Dserver（Ｃ１）を求める。この後コンテンツ管理サイト４は、乱数ｒ２を生成し、この乱数ｒ２はe-userを用いて暗号化される（Ｃ２＝Euser（ｒ２）を生成する）。この生成したｔ１およびＣ２をユーザ端末３に送信する。

【００６６】ユーザ端末３は、受け取ったｔ１が「ｔ１＝ｒ１」か否かを検証する。この検証で「ｔ１＝ｒ１」の場合には、秘密鍵ｄuserを用いてｔ２＝Duser（Ｃ２）を求める。このｔ２をユーザ端末３からコンテンツ管理サイト４に送信する。

【００６７】コンテンツ管理サイト４は、受け取ったｔ２が「ｔ２＝ｒ２」か否かを検証する。この検証で「ｔ２＝ｒ２」の場合に、セッション鍵Ｋを生成する。次に、コンテンツ管理サイト４は、このセッション鍵Ｋを公開鍵e-userを用いて暗号化する（Ｓ＝Euser（Ｋ）を生成する）。コンテンツ管理サイト４は、この暗号化したＳをユーザ端末３に送信する。

【００６８】ユーザ端末３は、秘密鍵duserを用いて、セッション鍵Ｋ＝Duser（Ｓ）を求め、このセッション鍵Ｋによってユーザ端末３とコンテンツ管理サイト４との間の情報伝送を実行する。

【００６９】このＡＫＥプロトコルの実行によって第三者による盗聴、否認、改造およびなりすましを防止できる。

【００７０】

【発明の効果】以上の説明から明らかなように、本発明のコンテンツ管理方法およびシステムによれば、コンテンツ管理サイトが一括してコンテンツ情報の案内を行っているので、ユーザに多大な手間と費用を負担させることなく、コンテンツ販売が容易に行われる。

【００７１】さらに、本発明によれば、ユーザ端末において使い勝手（利便性）に優れた購入コンテンツの使用管理が出来るという効果を奏する。

【００７２】さらに、本発明によれば、コンテンツ管理サイトにおいて、ユーザごとの個人情報が収集され、効果的なダイレクトマーケティングが可能になる。

【００７３】さらに、本発明によれば、ユーザは、所有する複数のユーザ端末のそれぞれごとに、コンテンツをダウンロードする必要がなくなり、その手間及び費用が削減される。

【００７４】さらに、本発明によれば、コンテンツ管理サイトからコンテンツの購入先が案内されるため、その購入先がユーザ側で容易に判明する。

【００７５】さらに、本発明によれば、購入した情報をコンテンツ管理サイトで保有しかつ管理することが出来るので、ユーザ側において、購入したコンテンツを、離れた場所の他のユーザ端末で取り込んで利用できる。

【００７６】さらに、本発明によれば、携帯端末の記憶容量が不足した場合に、携帯端末に格納されているコンテンツの使用権をコンテンツ管理サイトに移動させ、かつ、携帯端末に格納している情報を削除できるため、新たなコンテンツのダウンロードが可能になる。

【００７７】さらに、本発明によれば、コンテンツ管理サイトがコンテンツに広告などの情報を添付して携帯端末に転送するために、コンテンツ管理サイトは広告収入が得られるため、結果的にユーザのコンテンツ購入代金を低減できるようになる。

【００７８】さらに、本発明によれば、ＡＫＥ(Authentication And Key Exchange) プロトコルを用いた第三者認証を用いれば、盗聴（通信経路上での悪意あるデータ取得）、否認（通信相手先での通信の否定）、改造（通信経路上での第三者による伝送データの改変）、なりすまし（第三者が他人になりすましてデータ伝送を行う）

が防止できる。

【図面の簡単な説明】

【図１】　本発明の実施の形態１におけるシステム構成を示すブロック図である。

【図２】　本発明の実施の形態１におけるコンテンツ管理サイトの処理を説明するためのブロック図である。

【図３】　本発明の実施の形態１におけるユーザ登録、コンテンツ購入および購入コンテンツデータベース登録のシーケンス図である。

【図４】　本発明の実施の形態１におけるコンテンツ管理サイトからユーザへのコンテンツ使用権移動のシーケンス図である。

【図５】　本発明の実施の形態１におけるユーザからコンテンツ管理サイトへのコンテンツ使用権移動のシーケンス図である。

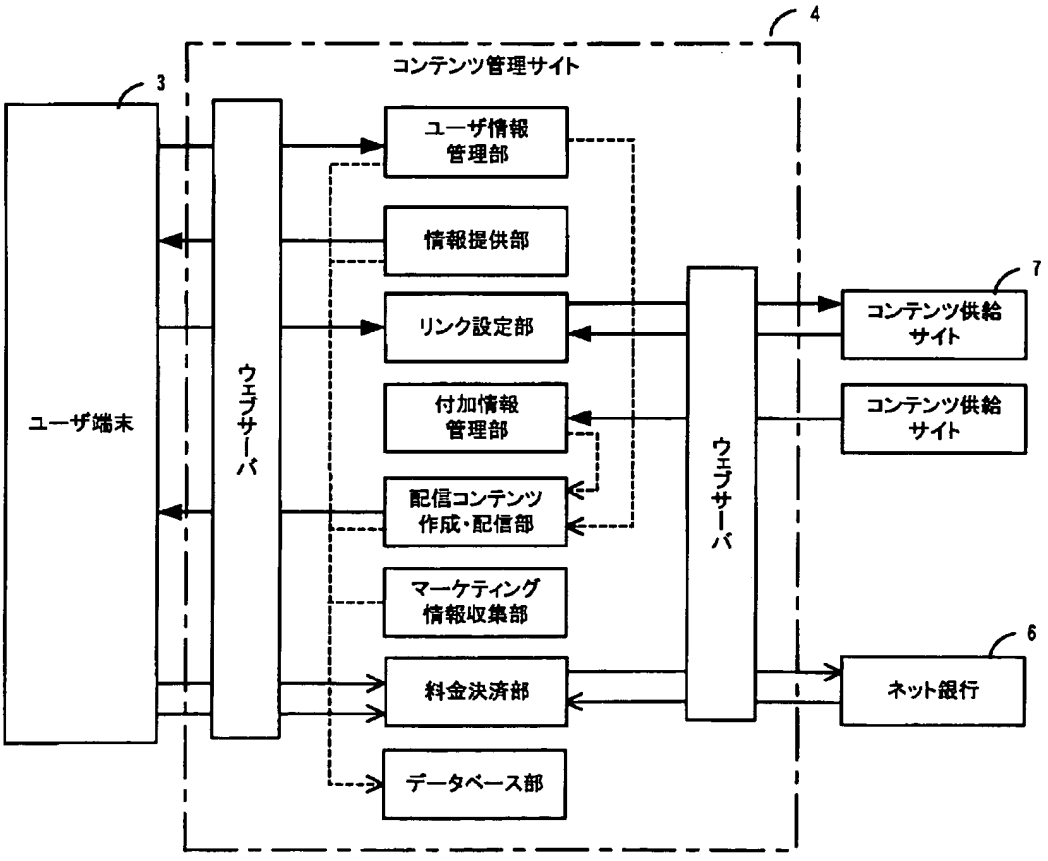
【図６】　本発明の実施の形態２におけるコンテンツ管＊理サイトの処理を説明するためのブロック図である。

【図７】　本発明の実施の形態３におけるコンテンツ管理サイトとユーザ端末間の相手認証とセッション鍵の共有を説明するためのシーケンス図である。

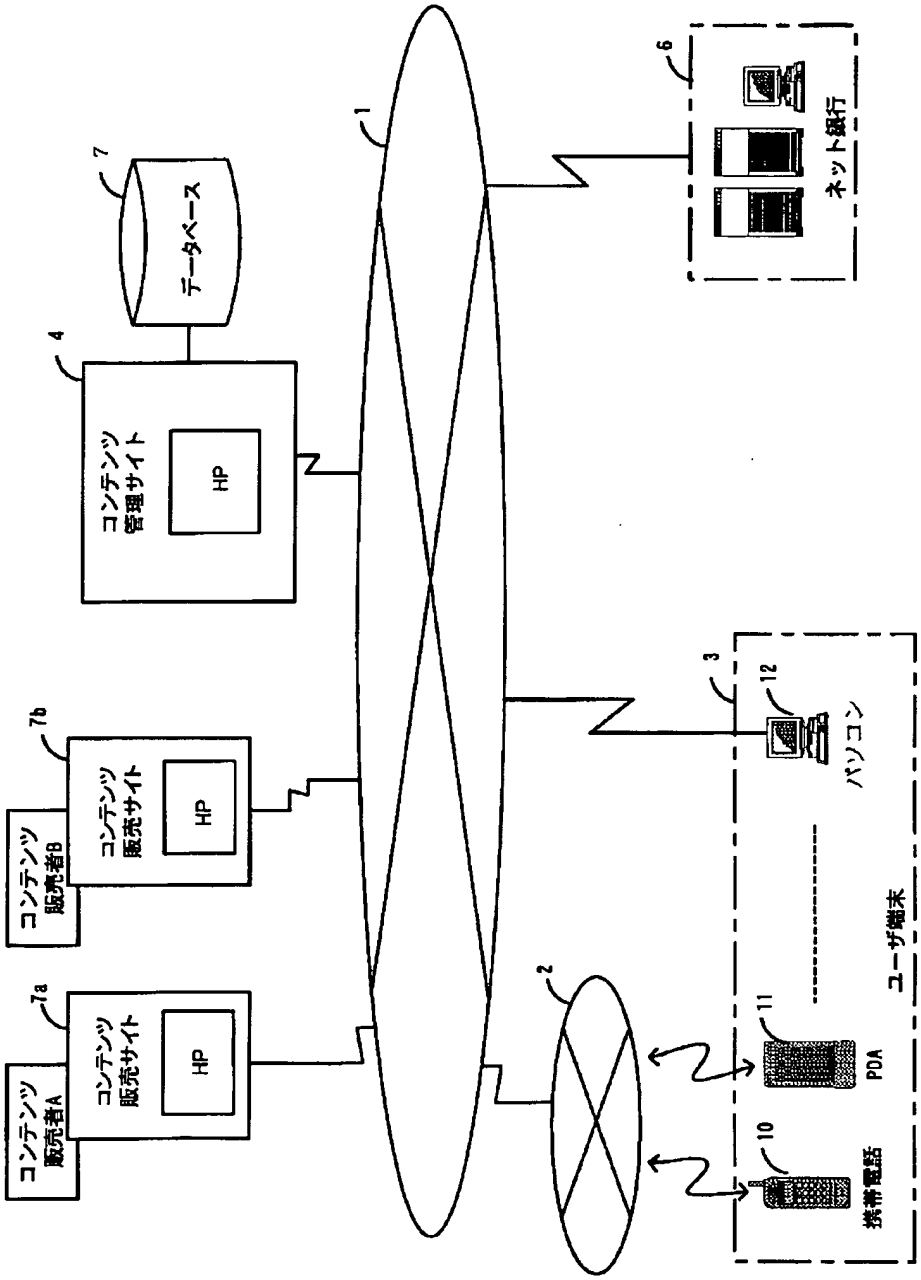
【符号の説明】

１　ディジタル固定通信網
２　ディジタル移動通信網
３　ユーザ端末
４　コンテンツ管理サイト
６　ネット銀行
７　コンテンツ供給サイト
８　データベース
１０　携帯電話機
１１　ＰＤＡ
１２　パソコン

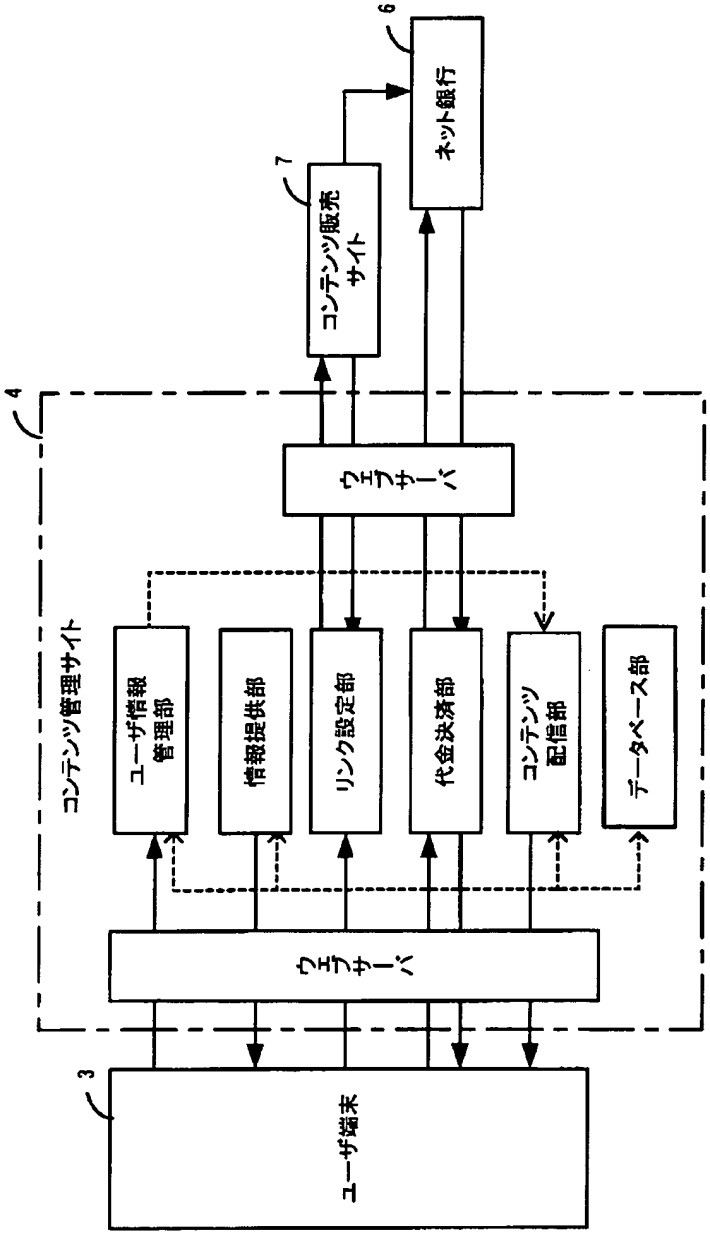
【図６】



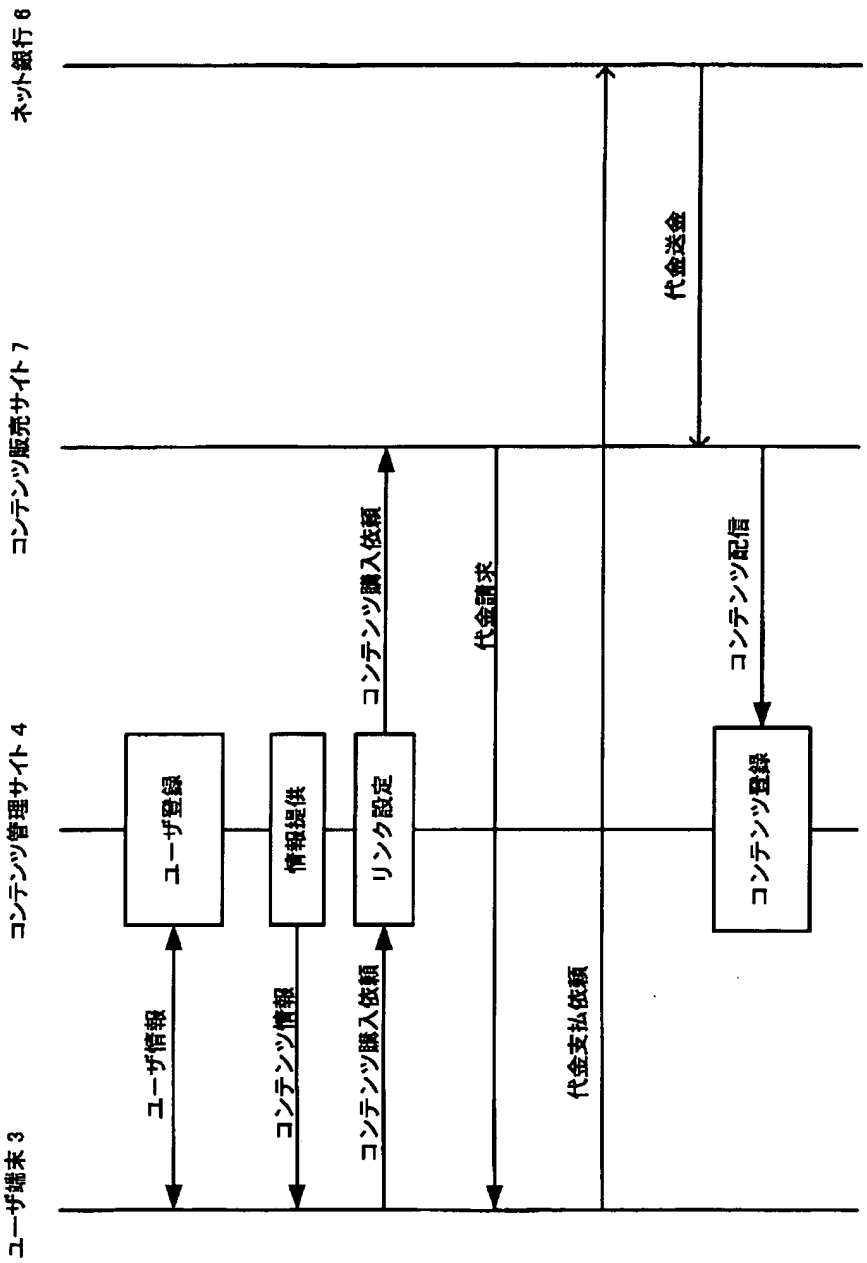
【図１】


1
2
3
4
6
7
7a
7b
データベース
コンテンツ管理サイト
HP
コンテンツ販売者A
コンテンツ販売サイト
コンテンツ販売者B
ネット銀行
パソコン
PDA
携帯電話
ユーザ端末
10
11
12

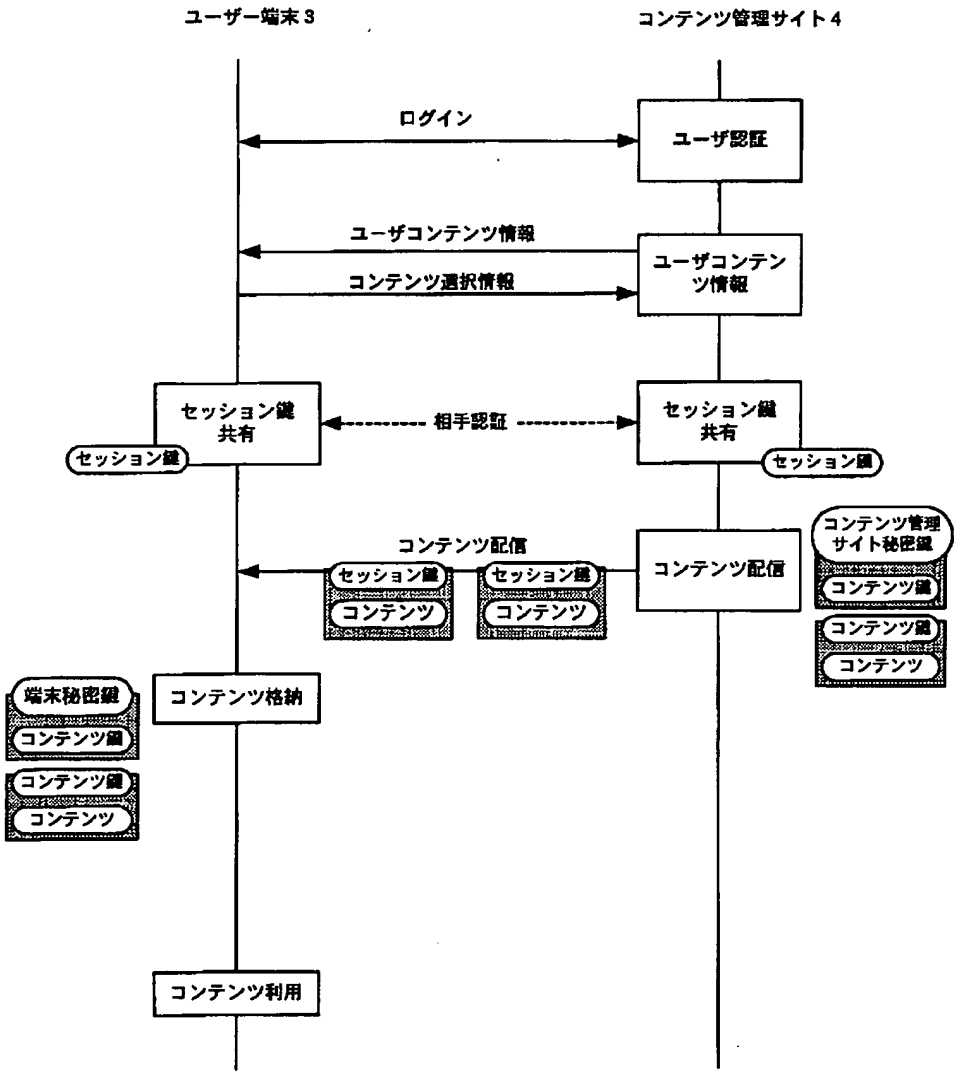
【図２】


6
ネット銀行
7
コンテンツ販売サイト
4
ウェブサーバ
コンテンツ管理サイト
ユーザ情報管理部
情報提供部
リンク設定部
代金決済部
コンテンツ配信部
データベース部
ウェブサーバ
3
ユーザ端末

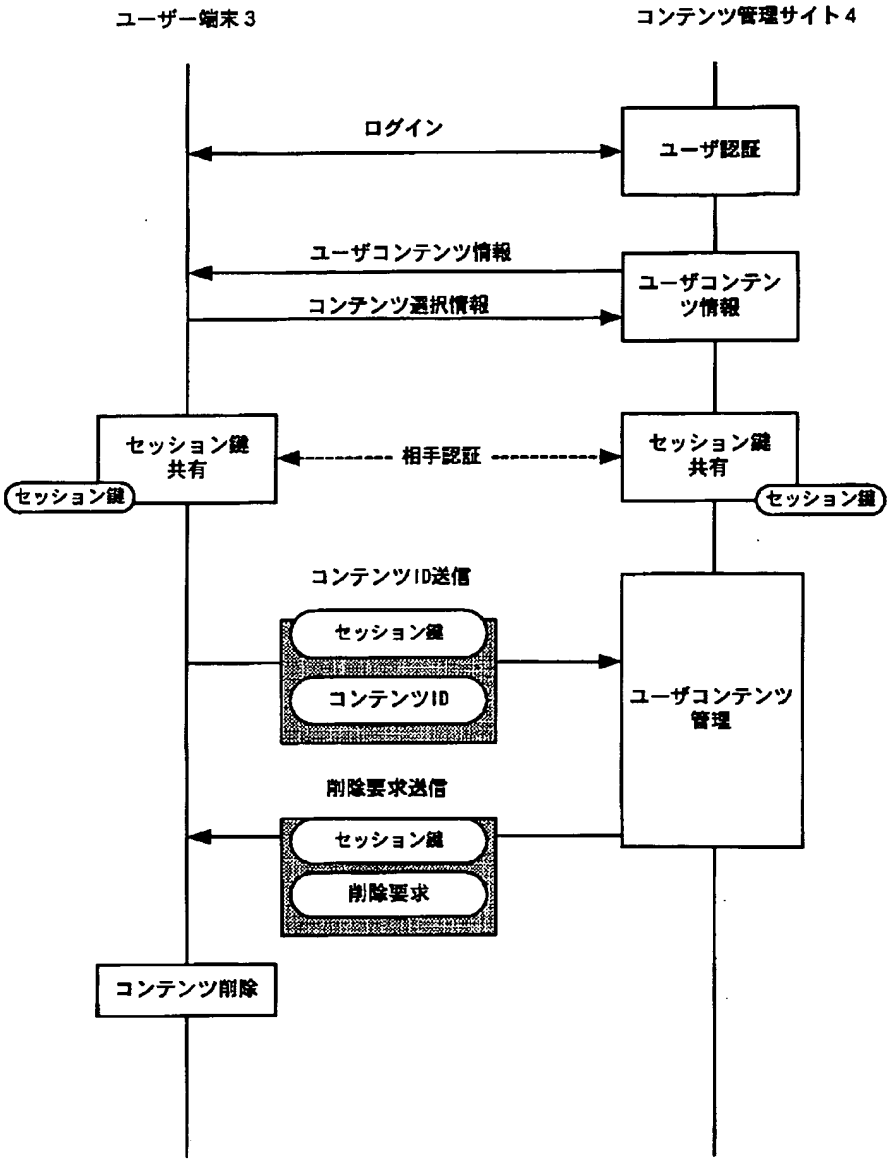
【図３】


ネット銀行 6
コンテンツ販売サイト 7
コンテンツ管理サイト 4
ユーザ端末 3
代金送金
コンテンツ購入依頼
代金請求
コンテンツ配信
ユーザ登録
情報提供
リンク設定
コンテンツ登録
ユーザ情報
コンテンツ情報
コンテンツ購入依頼
代金支払依頼

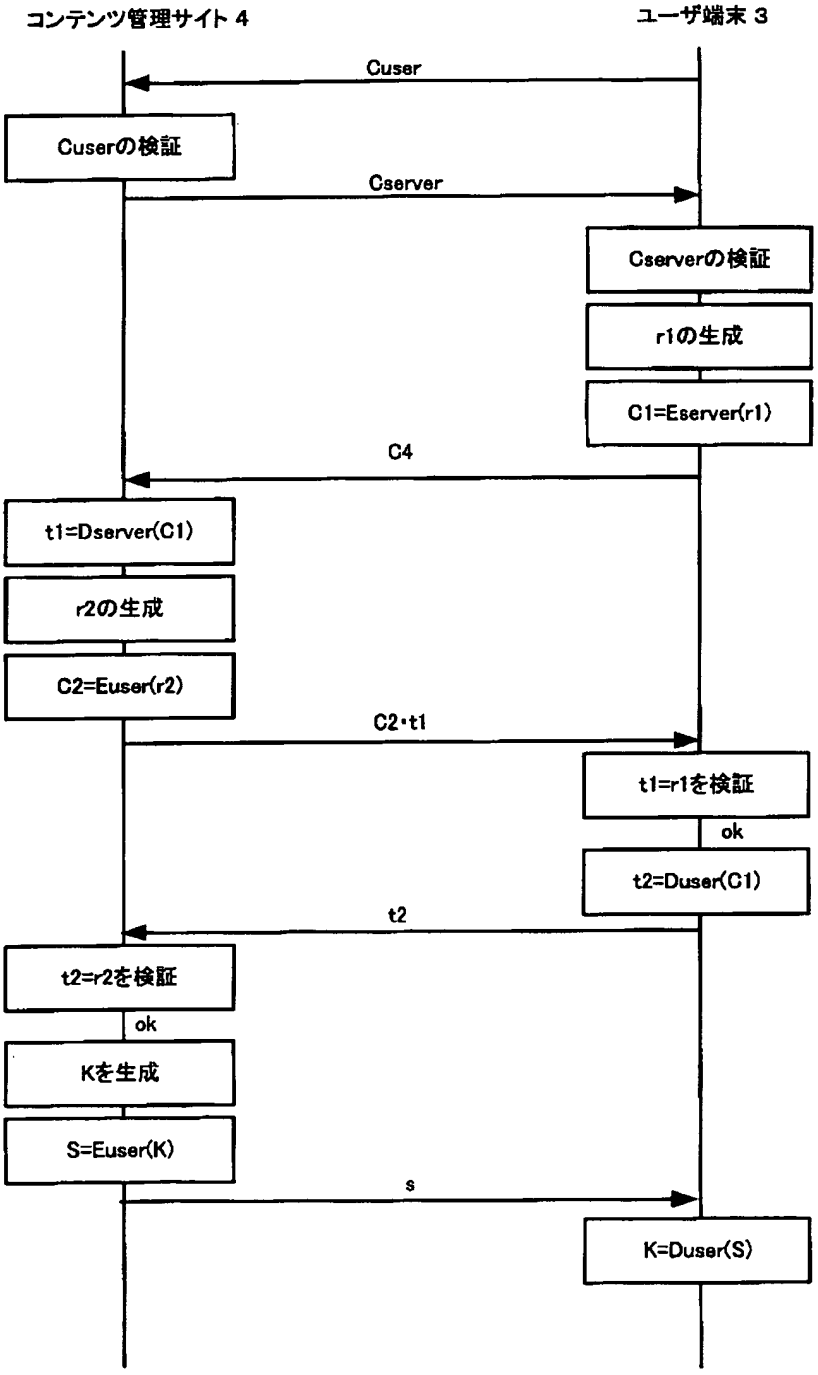
【図４】


ユーザー端末３
コンテンツ管理サイト４
ログイン
ユーザ認証
ユーザコンテンツ情報
コンテンツ選択情報
ユーザコンテンツ情報
セッション鍵共有
相手認証
セッション鍵共有
セッション鍵
セッション鍵
コンテンツ管理サイト秘密鍵
コンテンツ鍵
コンテンツ鍵
コンテンツ
コンテンツ配信
コンテンツ配信
セッション鍵
コンテンツ
セッション鍵
コンテンツ
端末秘密鍵
コンテンツ鍵
コンテンツ鍵
コンテンツ
コンテンツ格納
コンテンツ利用

【図５】


ユーザー端末３
コンテンツ管理サイト４
ログイン
ユーザ認証
ユーザコンテンツ情報
コンテンツ選択情報
ユーザコンテンツ情報
セッション鍵共有
相手認証
セッション鍵共有
セッション鍵
セッション鍵
コンテンツID送信
セッション鍵
コンテンツID
ユーザコンテンツ管理
削除要求送信
セッション鍵
削除要求
コンテンツ削除

【図７】



フロントページの続き

(51)Int.Cl.[7]	識別記号	F I		ﾃｰﾏｺｰﾄﾞ(参考)
H04L 9/08		H04L 9/00	601A	
			601B	

６０１Ｅ

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-269375

(43)Date of publication of application : 20.09.2002

---

(51)Int.Cl. G06F 17/60
H04L 9/08

---

(21)Application number : 2001-070580 (71)Applicant : SONY CORP

(22)Date of filing : 13.03.2001 (72)Inventor : NAGAI KIKO

---

(54) CONTENTS MANAGEMENT METHOD AND SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contents management method and its system allowing a user to easily and safely purchase contents for use from a contents supply site.

SOLUTION: From a user terminal 3, user registration is carried out in a contents management site 4, and the user purchase the contents after viewing them on a homepage of the contents management site 4 and makes a payment of a purchase charge for the contents via an Internet bank. The contents management site 4 registers the contents in a database 8 and transmits an information license and the contents to the user terminal. On the basis of the transferred license, the user terminal incorporates the contents to use them. The user terminal can return the contents license to the contents management site 4 and delete the held contents. The user can download the information for use again from the contents management site 4 on the

basis of the license.

CLAIMS

[Claim(s)]

[Claim 1]A contents management method which manages contents provided with a contents supply site, a contents management site, and a user terminal by which the purchase of contents was recommended and purchased, comprising:

A step to which a user terminal registers for a contents supply site as a user.

A step which a contents supply site shows the contents of contents to a user terminal.

A step to which a user terminal purchases contents from a contents supply site.

A step which pays a price for contents which a user terminal purchased to a contents supply site.

A step to which a contents supply site registers into a database of a contents management site information which a user terminal purchased.

A step to which a contents supply site makes a user terminal move a contents royalty registered into a database.

A step into which a user terminal incorporates contents from a contents supply site based on a contents royalty.

[Claim 2]The contents management method according to claim 1, wherein said

user terminal has further a step which eliminates information which a incorporated contents royalty was returned to a contents management site, and was incorporated with a user terminal.

[Claim 3]The contents management method according to claim 2, wherein said user terminal has further a step which incorporates contents returned to a contents management site above based on a contents royalty.

[Claim 4]The contents management method according to claim 1 with which a contents supply site is characterized by contents which present the contents of contents to a user terminal being a contents list and the contents of contents as which purchase is recommended at least.

[Claim 5]The contents management method according to claim 1, wherein a user terminal registers a user's various personal information into direct marketing at least with user-identification numerals and a password in a step which registers for said contents supply site as a user.

[Claim 6]The contents management method according to claim 1 when said contents management site incorporates [a user terminal] contents from a contents management site, wherein it has further a step which attaches information including an advertisement to contents.

[Claim 7]The contents management method according to claim 1, wherein information on said royalty is enciphered and transmitted with an identification signal and a password in user registration between said contents supply site and a user terminal.

[Claim 8]Said encryption is AKE (Authentication And Key Exchange). The contents management method according to claim 7, wherein a protocol is applied.

[Claim 9]In a content management system which manages contents provided with a contents supply site, a contents management site, and a user terminal by which the purchase of contents was recommended and purchased, Based on a demand, said contents supply site accumulates contents, supplies them to a contents management site, and said user terminal, Perform user registration for purchasing contents, and contents are incorporated with a royalty of purchased contents, Based on a royalty of contents, incorporate contents again, and a contents management site, When said user terminal registers as a user, contents are incorporated and memorized from a contents supply site, A content management system moving a contents royalty to said user terminal based on a demand from a user terminal, and supplying said memorized contents to said

user terminal.

[Claim 10]The content management system according to claim 9, wherein said user terminal eliminates information which a incorporated contents royalty was returned to a contents management site, and was incorporated with a user terminal.

[Claim 11]The content management system according to claim 10, wherein said user terminal incorporates further contents returned to a contents management site above with a contents royalty.

[Claim 12]The content management system according to claim 9 having further a net payment means for performing a payment between said user terminal and a contents management site or between said user terminal and a contents supply site.

[Claim 13]When said user terminal registers for said contents supply site as a user, said contents management site with user-identification numerals and a password. The content management system according to claim 9 registering a user's various personal information into direct marketing at least.

[Claim 14]The contents management method according to claim 9 when said contents management site incorporates [said user terminal] contents from said

contents management site, wherein it attaches information including an advertisement to contents.

[Claim 15]The content management system according to claim 9, wherein said contents management site is provided with a database for storing a royalty of contents and contents at least.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]this invention -- the communication network (intranet.) under TCP/IP environment The Internet, an extra network, a UNIX (registered trademark) workstation, the following and the Internet -- saying -- it leads and is related with the contents management method and system for managing use of the contents by which the purchase of information (for example, the contents of contents, such as music, a still picture, and an animation, and henceforth [contents]) was recommended and purchased.

[0002]

[Description of the Prior Art]Conventionally, the contents of music, a still picture, and an animation, etc. are provided in the communication network under TCP/IP

environment. These contents are downloaded and used with the user terminal (a small general purpose computer and the personal digital assistant in which Internet surfing is possible) which carries a web browser.

[0003]When it provides these contents on a website, and when a user uses, the software which stored the copyright module in the user site is used from the position of copyright protection. The contents royalty downloaded by such a copyright module is bound to the user terminal which performed download.

[0004]

[Problem(s) to be Solved by the Invention]Contents are provided through such a website and there are the respectively following problems in the contents providing site of the position of managing the copyright, and the user terminal which acquires and uses contents.

[0005](1) Contents providing site (a) When the website which provides many and unspecified users with information provides contents, the management including the advertisement (for example, magazine advertising and search engine banner advertising) to the user takes great time and expense.

(b) When the user is using two or more terminals, music etc. must be downloaded for each user terminal of every from the relation of copyright. If it

puts in another way, a user terminal will be forced the burden of time and effort and expense, and it will become a hindrance factor through which contents are spread as a result.

[0006](2) When using the same contents at two or more terminals which one user terminal (a) person's user owns, in each of two or more of the terminals, the same contents will be downloaded and used from a website. In this case, operation will be troublesome and that download expense will increase.

[0007](b) If the storage capacities of a user terminal run short, in order to download new contents, it is necessary to delete the contents currently kept before. It may stop being able to reproduce the contents which abnormalities are generating and keeping to the user terminal. In this case, it is necessary to back up the downloaded contents to recording media (an external hard disk device, a floppy (registered trademark) disk, MO, etc.) or, download for the second time will be performed, and that time and effort and purchase expense will be required.

[0008](c) The website which provides much various contents is on the Internet. That is, the website of the acquisition place of the contents for which a user asks does not become clear easily. In this case, a user will investigate a journal, or

the search and the inspection by Internet surfing will be needed, and that time and effort will be taken, and expense will also increase.

(e) It was difficult to incorporate and use the downloaded contents which are kept by the user terminal with other user terminals at the distant place, for example, a place where one has gone, and it was inconvenient.

[0009]In [are made in order that the purpose of this invention may solve the technical problem in such conventional technology, are a thing, and] a contents providing site, The recommendation of content purchase can be performed easily and it is in providing the contents management method and system whose user-friendliness (convenience) of the purchased contents use management improves in a user terminal.

[0010]

[Means for Solving the Problem]In order to attain an aforementioned problem, according to the invention according to claim 1, this invention is provided with a contents supply site, a contents management site, and a user terminal, and is characterized by that a contents management method which manages contents by which the purchase of contents was recommended and purchased comprises the following.

A step to which a user terminal registers for a contents supply site as a user.

A step which a contents supply site shows the contents of contents to a user terminal.

A step to which a user terminal purchases contents from a contents supply site.

A step which pays a price for contents which a user terminal purchased to a contents supply site, A step to which a contents supply site registers into a database of a contents management site information which a user terminal purchased, A step which a contents supply site makes move a contents royalty registered into a database to a user terminal, and a step into which a user terminal incorporates contents from a contents supply site based on a contents royalty.

[0011]According to the invention according to claim 2, a user terminal of this invention returns a incorporated contents royalty to a contents management site, and it has further a step which eliminates information incorporated with a user terminal.

[0012]According to the invention according to claim 3, a user terminal of this invention has further a step which incorporates contents returned to a contents

management site based on a contents royalty.

[0013]According to the invention according to claim 4, contents which a contents supply site of this invention shows the contents of contents to a user terminal are characterized by being a contents list and the contents of contents as which purchase is recommended at least.

[0014]According to the invention according to claim 5, in a step to which a user terminal registers for a contents supply site as a user, this invention registers a user's various personal information into direct marketing at least with user-identification numerals and a password.

[0015]According to the invention according to claim 6, a contents management site of this invention has further a step which attaches information including an advertisement to contents, when a user terminal incorporates contents from a contents management site.

[0016]According to the invention according to claim 7, information on a royalty of this invention is enciphered and transmitted with an identification signal and a password in user registration between a contents supply site and a user terminal.

[0017]According to the invention according to claim 8, encryption of this invention is AKE (Authentication AndKey Exchange). A protocol is applied.

[0018]In a content management system which manages contents by which according to the invention according to claim 9 this invention was provided with a contents supply site, a contents management site, and a user terminal, and the purchase of contents was recommended and purchased, Based on a demand, a contents supply site accumulates contents, supplies them to a contents management site, and said user terminal, Perform user registration for purchasing contents, and contents are incorporated with a royalty of purchased contents, Based on a royalty of contents, incorporate contents again, and a contents management site, When a user terminal registers as a user, incorporate and memorize contents from a contents supply site, and a contents royalty is moved to a user terminal based on a demand from a user terminal, and said memorized contents are supplied to a user terminal.

[0019]According to the invention according to claim 10, a user terminal of the invention according to claim 9 returns a incorporated contents royalty to a contents management site, and it eliminates information incorporated with a user terminal.

[0020]According to the invention according to claim 11, a user terminal of the invention according to claim 10 incorporates further contents returned to a

contents management site with a contents royalty.

[0021]According to the invention according to claim 12, the invention according to claim 9 is further provided with a net payment means for performing a payment between a user terminal and a contents management site or between a user terminal and a contents supply site.

[0022]According to the invention according to claim 13, a contents management site of the invention according to claim 9, When a user terminal registers for a contents supply site as a user, a user's various personal information is registered into direct marketing at least with user-identification numerals and a password.

[0023]According to the invention according to claim 14, a contents management site of the invention according to claim 9 attaches information including an advertisement to contents, when a user terminal incorporates contents from said contents management site.

[0024]According to the invention according to claim 15, a contents management site of the invention according to claim 9 is provided with a database for storing a royalty of contents and contents at least.

[0025]

[Embodiment of the Invention]The contents management method and system of

embodiment 1., next the embodiment of the invention 1 are explained in detail with reference to drawings. Drawing 1 is a block diagram showing the system configuration in the embodiment of the invention 1. In drawing 1, in order to realize this invention, it has the composition of the communication network (Internet) under TCP/IP environment.

[0026]The communication network shown in drawing 1 has the digital-mobile-communication network 2 connected to this digital point-to-point-communication network 1 with the digital point-to-point-communication network 1 of ISDN (Integrated Services Digital Network). The digital-mobile-communication network 2 has a base station which is not illustrated, and personal digital assistants, such as many portable telephones 10 which carry the web browser in which an Internet access is possible in this base station, and PDA(Personal Digital Assistant) 11, are connected on radio.

[0027]The contents management site 4 which manages the right (royalty) for a user terminal to use management of contents and contents is connected to the digital point-to-point-communication network 1. The personal computer 12 to which the database 8 which memorizes contents etc. is connected in the

contents management site 4 and which a user uses further, The net bank 6 as a net payment means of communication installed in a bank, a credit card company, etc. for performing various kinds of payments explained henceforth is formed.

[0028]The contents supply site 7 (7a, 7b) which the contents selling persons A and B who provide contents, such as a still picture, an animation, and music, according to the demand from the contents management site 4 have is established in the communication network shown in drawing 1. Here, although the contents supply site 7 shows only two for convenience' sake, these may be two or more.

[0029]The module of encryption processing (for example, AKE protocol explained in detail below) is carried so that the personal digital assistant 3 may be explained in detail henceforth. This module is realized by a digital signal processor (DSP) and software, for example.

[0030]The contents which downloaded and came to hand in this personal digital assistant 3 are reproduced, For example, the program for reproducing the downloaded music data and managing contents is stored, and this program is provided also with GUI (Graphical User Interface) for making directions processing about contents, etc. easy.

[0031]Hereafter, the outline of the system configuration of this invention is explained briefly. Drawing 2 is a block diagram for explaining the outline of the system configuration of this invention. In drawing 2, the connecting relation of the personal digital assistant 3, the contents management site 4, the contents selling site 5, and the net bank 6 is shown.

[0032]The personal digital assistant 3 communicates between the contents management sites 4, the contents management site 4 communicates between the contents supply sites 7, and the personal digital assistant 3 performs charge settlement between the net banks 6 via the contents management site 4.

[0033]The contents management site 4 contains (1) User Information Management Department, (2) offer-of-information parts, (3) link setting parts, (4) payment parts, (5) contents distribution parts, (6) database sections, etc.

[0034]As mentioned above, main processings of this invention are performed in the contents management site 4. Below, processing of the contents management site 4 shown in drawing 2 is explained in detail using the sequence diagram of drawing 5 from drawing 3.

[0035]<User registration, content purchase, and purchase contents database registration> drawing 3 is a sequence diagram of user registration, content

purchase, and purchase contents database registration processing. In drawing 3, first, the user terminal 3 accesses the contents management site 4, and performs information inputting (for example, personal information, such as taste of an address, a name, and an individual) for registering User Information on the homepage of the contents management site 4. The contents management site 4 registers User Information. Here, various kinds of items are registered at the User Information Management Department which explained user registration by drawing 2. An example of the item registered is shown table 1. This item is an example and may register other items.

[0036]

[Table 1]

[0037]The information for direct marketing for every user of a user terminal is also collectable in the database 8. By this gathering information, the personal

information for every user is collected and effective direct marketing becomes possible.

[0038]Next, the contents management site 4 presents the contents information to sell on a homepage (H.P.). This contents information is performed in the offer-of-information part explained by drawing 2. A user terminal peruses this homepage.

[0039]Then, the information on a desired contents purchase request (for example, bar code) is transmitted with user-identification numerals and a password from a user terminal. When the contents management site 4 has recognized user-identification numerals and a password, it stretches the link of the contents management site 4 and the contents selling site 7 in the link setting part of drawing 2, and transmits the purchase request from the user terminal 3 to the contents selling site 7.

[0040]The contents selling site 7 which received the purchase request notifies the sales amount of contents to the user terminal 3 with an E-mail directly. It may be made to perform this notice of contents invoicing to the user terminal 3 via the contents management site 4 from the contents selling site 7.

[0041]Via the payment part explained by drawing 2, the user terminal 3 which

received the notice of invoicing sets a link to the net bank 6, and performs remittance of 7 to a contents selling site. A credit card can also perform this settlement of accounts. The user terminal 3 links to the net bank 6 directly, and it may be made to perform the settlement of accounts by the change of a debit card or electronic money.

[0042]After this payment, the contents selling site 7 transmits the purchased contents in the contents management site 4. The contents management site 4 stores the contents which the user terminal 3 purchased in the database 8 put on the contents management site 4 by processing of the database section of drawing 2. In this case, user-identification numerals and a password are made to correspond, and purchase contents are stored in the database 8.

[0043]<Move of contents royalty from contents management site 4 to personal digital assistant 3> drawing 4 is a sequence diagram which moves a contents royalty to the personal digital assistant 3 from the contents management site 4. In drawing 4, the outline of processing in which a user terminal incorporates the user contents and the contents royalty which are stored in the database 8 of the contents management site 4, and the personal digital assistant 3 uses the incorporated contents is shown.

[0044]In this processing, login is first performed from the user terminal 3 to the contents management site 4. In this login, a user enters user-identification numerals and a password on the homepage of the contents management site 4, after accessing the contents management site 4 from the user terminal 3.

[0045]The contents management site 4 will transmit the information about a user's contents held on the database 8, including for example, a contents name, a contents creator, a purchase place, the move propriety of a royalty, etc., to the user terminal 3, if user-identification numerals and a password are recognized correctly. The user terminal 3 chooses desired contents from the user contents information displayed on the screen, and transmits the selected contents selection information to the contents management site 4.

[0046]Next, mutual recognition using an AKE protocol is performed between the user terminal 3 and the contents management site 4, for example, and processing which shares a session key is performed. The mutual recognition by use of this AKE protocol is mentioned later.

[0047]Next, in the contents management site 4, the contents key of user contents is enciphered with the generated session key. The contents enciphered with this enciphered contents key and contents key are transmitted to a user

terminal.

[0048]Next, in the user terminal 3, the enciphered contents key is decrypted with the session key shared with the aforementioned contents management site 4, a contents key is taken out, and it enciphers again with a secret key, and memorizes in the memory in the user terminal 3 etc. which are not illustrated. The contents enciphered with the contents key are also memorized by the memory in the user terminal 3 etc. which are not illustrated.

[0049]In the personal digital assistant 3, a user uses the contents memorized by the memory. In this case, contents are reproduced by the software for user contents managing (program) beforehand installed in the user terminal 3. This program decrypts the enciphered contents key, decrypts the enciphered contents using the contents key acquired by this decryption, and performs a screen display, a music output, etc. of contents.

[0050]As a result, it becomes unnecessary for a user to download and use the same contents for two or more user terminals 3 to own, and that time and effort and expense are reduced.

[0051]The user terminal 3 incorporates the contents royalty purchased through the contents management site 4 with the user terminal of the distant place, and

can be used now.

[0052]<Move of contents royalty from personal digital assistant 3 to contents management site 4> drawing 5 is a sequence diagram showing movement of a contents royalty to the contents management site 4 from the personal digital assistant 3. In drawing 5, the storage capacity of the memory in a user terminal is insufficient, for example, When incorporation of new contents cannot be performed, the user terminal 3 deletes the contents incorporated from the contents management site 4, and moves a contents royalty to the contents management site 4 temporarily.

[0053]In this processing, login is first performed from the user terminal 3 in the contents management site 4. In this login, a user accesses the contents management site 4 from the user terminal 3, and enters user-identification numerals and a password on that homepage.

[0054]The contents management site 4 will transmit the information about a user's contents held on the database 8 to the user terminal 3 from the contents management site 4, if this user-identification numerals and password are recognized correctly. In the user terminal 3, desired contents are chosen from the user contents information which carried out a screen display, and the

selected contents selection information is transmitted to the contents management site 4.

[0055]Next, mutual recognition using an AKE protocol is performed between the user terminal 3 and the contents management site 4, for example, and processing which shares a session key is performed. The mutual recognition by use of this AKE protocol is mentioned later.

[0056]Next, in the personal digital assistant 3, with the generated session key, contents identification signal ID which determines user contents uniquely is enciphered, and it transmits to the contents management site 4. On the other hand, the contents management site 4 transmits a contents deletion request to the user terminal 3.

[0057]The user terminal 3 which received this contents deletion request deletes the contents key and contents which were stored in the internal memory etc.

[0058]Thus, when a storage capacity is insufficient for the user terminal 3, download of new contents is attained by deleting the contents which make it move to the contents management site 4, and store the stored contents royalty.

[0059]Embodiment 2. drawing 6 is a block diagram for explaining the outline of the processing in other embodiments of this invention. In the processing in

drawing 6, information attachment service and direct marketing information are collected. In drawing 6, it adds to (6) database sections from (1) User Information Management Department which showed drawing 2, and the additional information Management Department and a direct marketing information gathering part are newly included. In addition to processing of drawing 2, in drawing 6, the contents management site 4 performs the next processing.

The <additional information management> contents management site 4 stores in the database 8 of the contents management site 4 the additional information about the information provided from the contents supply site 7, for example, an advertisement, and contents. The contents management site 4 attaches and distributes ********** stored in the additional information Management Department to the contents to which the personal digital assistant 3 distributes.

[0060]The income according [the contents management site 4] to advertisement information distribution is obtained by this. The price for content purchase for a user can be reduced as a result.

[0061]A user collects the information on the kind of contents purchased through the contents management site 4, purchase time, a purchase time belt, etc., and

stores the <collection processing of direct marketing information> contents management site 4 in the database 8.

[0062]The gathering information of this purchase time, a purchase time belt, etc. is supplied to the contents supply site 7, or is used in the contents management site 4. This. The contents management site 4 and the contents supply site 7 can know the tendency etc. of the contents which a user purchases.

[0063]Embodiment 3.

<Sharing of contents management site, partner attestation [between user terminals], and session key> drawing 7 is a sequence diagram for explaining sharing of the partner attestation by the AKE protocol between the contents management site 4 and the user terminal 3, and a session key in detail. In drawing 7, the user terminal 3 transmits user certificate Cuser published by the third party's certifying authority to the contents management site 4. The contents management site 4 checks the right or wrong of user certificate Cuser from the user terminal 3.

[0064]Next, the contents management site 4 transmits the certificate Cserver published by the third party's certifying authority to the user terminal 3. The user terminal 3 verifies the right or wrong of the certificate Cserver. In the user

terminal 3, this verification gains public key e-server of the contents management site 4 from the certificate Cserver to a right case. Next, the user terminal 3 generates the random number r1, and this random number r1 is enciphered using public key e-server (C1=Eserver (r1) is generated).

[0065]The user terminal 3 transmits the encryption C1 to the contents management site 4. The contents management site 4 calculates t1=Dserver (C1) using the secret key dserver. After this, the contents management site 4 generates the random number r2, and this random number r2 is enciphered using e-user (C2=Euser (r2) is generated). These t1 and C2 that were generated are transmitted to the user terminal 3.

[0066]The user terminal 3 verifies whether t1 received is "t1=r1." In the case of "t1=r1", t2=Duser (C2) is calculated using the secret key duser by this verification. These t2 is transmitted to the contents management site 4 from the user terminal 3.

[0067]The contents management site 4 verifies whether t2 received is "t2=r2." In the case of "t2=r2", session key K is generated by this verification. Next, the contents management site 4 enciphers this session key K using public key e-user (S=Euser (K) is generated). The contents management site 4 transmits

this enciphered S to the user terminal 3.

[0068]Using the secret key duser, the user terminal 3 calculates session key K=Duser (S), and performs information transmission between the user terminal 3 and the contents management site 4 by this session key K.

[0069]Tapping by a third party, denial, reconstruction, and spoofing can be prevented by execution of this AKE protocol.

[0070]

[Effect of the Invention]Contents selling is performed easily, without making a user pay great time and effort and expense, since the contents management site is guiding contents information collectively according to the contents management method and system of this invention so that clearly from the above explanation.

[0071]According to this invention, the effect that use management of the purchase contents which were excellent in user-friendliness (convenience) in the user terminal can be performed is done so.

[0072]According to this invention, in a contents management site, the personal information for every user is collected and effective direct marketing becomes possible.

[0073]According to this invention, it becomes unnecessary for a user to download contents for every each of two or more user terminals to own, and the time and effort and expense are reduced.

[0074]According to this invention, since the purchase place of contents is guided from a contents management site, the purchase place becomes clear easily by the user side.

[0075]According to this invention, since the purchased information can be held and managed in a contents management site, the purchased contents can be incorporated and used for the user side with other user terminals of the distant place.

[0076]According to this invention, since the information which is made to move the royalty of the contents stored in the personal digital assistant to a contents management site, and is stored in a personal digital assistant can be deleted when the storage capacities of a personal digital assistant run short, download of new contents is attained.

[0077]According to this invention, in order that a contents management site may attach advertising information to contents and may transmit to a personal digital assistant, since advertising revenue is obtained, the contents management site

can reduce the price for content purchase for a user as a result.

[0078]According to this invention, it is AKE (Authentication And Key Exchange). If the third party certificate using a protocol is used, Tapping (malicious data acquisition on a communication path), denial (denial of communication at the communications-partner point), reconstruction (change of the transmission data by the third party on a communication path), and spoofing (a third party becomes others, clears up and performs data communications) can be prevented.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a block diagram showing the system configuration in the embodiment of the invention 1.

[Drawing 2]It is a block diagram for explaining processing of the contents management site in the embodiment of the invention 1.

[Drawing 3]It is a sequence diagram of the user registration in the embodiment of the invention 1, content purchase, and purchase contents database registration.

[Drawing 4]It is a sequence diagram of contents royalty movement from the contents management site in the embodiment of the invention 1 to a user.

[Drawing 5]It is a sequence diagram of contents royalty movement to the

contents management site in the embodiment of the invention 1 from a user.

[Drawing 6]It is a block diagram for explaining processing of the contents management site in the embodiment of the invention 2.

[Drawing 7]It is a sequence diagram for explaining the contents management site in the embodiment of the invention 3, the partner attestation between user terminals, and sharing of a session key.

[Description of Notations]

1 Digital point-to-point-communication network

2 Digital-mobile-communication network

3 User terminal

4 Contents management site

6 Net bank

7 Contents supply site

8 Database

10 Portable telephone

11 PDA

12 Personal computer